MICHAEL GREGG

Cert Guide

Learn, prepare, and practice for exam success

CEH

Certified Ethical Hacker

PEARSON IT CERTIFICATION

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Certified Ethical Hacker (CEH) Cert Guide

Michael Gregg

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

Certified Ethical Hacker (CEH) Cert Guide

Copyright © 2014 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5127-0

ISBN-10: 0-7897-5127-5

Library of Congress Control Number: 2013953303

Printed in the United States of America

First Printing: December 2013

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearsoned.com

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Kathy Ruiz

Technical Editors
Brock Pearson
Tatyana Zidarov

Publishing Coordinator
Vanessa Evans

Media Producer
Lisa Matthews

Book Designer
Alan Clements

Compositor
Jake McFarland

Contents at a Glance

Table of Contents

About the Author

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTT+, A+, N+, Security+, CCNA, CASP, CISA, CISM, CEH, CHFI, and GSEC) is the founder and president of Superior Solutions, Inc., a Houston, Texas-based IT security consulting firm. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the country to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-authoring the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-authored 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (Wiley, 2008); *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (Syngress, 2006); *Certified Ethical Hacker Exam Prep 2* (Que, 2006); and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams, 2005).

Michael has been quoted in newspapers such as the *New York Times* and featured on various television and radio shows, including NPR, ABC, CBS, Fox News, and others, discussing cyber security and ethical hacking. He has created more than a dozen IT security training security classes. He has created and performed video instruction on many security topics, such as cyber security, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and has a slot in his garage for a new project car.

You can reach Michael by email at MikeG@thesolutionfirm.com.

Dedication

In loving memory of my mother-in-law, Elvira Estrello Cuellar, who always stood behind me, encouraged me, and prayed that all my dreams would come true.

Acknowledgments

I would like to offer a big "thank you" to Christine, for her help and understanding during the long hours that such a project entails. I also want to thank Curley, Betty, Gen, Alice, and all of my family. A special thanks to the people of Pearson IT Certification, who helped make this project a reality, including Betsy Brown. I would also like to thank my technical editors, Brock Pearson and Tatyana Zidarov.

Finally, I would like to acknowledge all the dedicated security professionals who contributed "In the Field" elements for this publication. They include Darla Bryant, Guy Bruneau, Ron Bandes, Jim Cowden, Laura Chappell, Rodney Fournier, Pete Herzog, Bryce Gilbrith, George Mays, Mark "Fat Bloke" Osborn, Donald L. Pipkin, Shondra Schneider, and Allen Taylor.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email:	feedback@pearsonitcertification.com
Mail:	Pearson IT Certification ATTN: Reader Feedback 800 East 96th Street Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

The EC-Council Certified Ethical Hacker (CEH) exam has become the leading ethical hacking certification available today. CEH is recognized by both employers and the industry as providing candidates with a solid foundation of hands-on security testing skills and knowledge. The CEH exam covers a broad range of security concepts to prepare candidates for the technologies that they are likely to be working with if they move into a role that requires hands-on security testing.

Let's talk some about what this book is. It offers you a one-stop shop for what you need to know to pass the exam. You do not have to take a class in addition to buying this book to pass the exam. However, depending on your personal study habits or learning style, you might benefit from buying this book *and* taking a class.

Cert Guides are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the Cert Guides reflects the nature of the CEH certification exam. The Cert Guides provide you with the factual knowledge base you need for the exams, and then take it to the next level with exercises and exam questions that require you to engage in the analytic thinking needed to pass the CEH exam.

EC-Council recommends that the typical candidate for this exam have a minimum of 2 years of experience in IT security. In addition, EC-Council recommends that candidates have preexisting knowledge of networking, TCP/IP, and basic computer knowledge.

Now let's briefly discuss what this book is not. It is not a book designed to teach you advanced hacking techniques or the latest hack. This book's goal is to prepare you for the CEH 312-50 exam, and it is targeted to those with some networking, OS, and systems knowledge. It provides basics to get you started in the world of ethical hacking and prepare you for the exam. Those wanting to become experts in this field should be prepared for additional reading, training, and practical experience.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CEH exam (312-50). In fact, if the primary objective of this book was different, the book's title would be misleading; however, the methods used in this book to help you pass the CEH exam are designed to also make you much more knowledgeable about how penetration testers do their job. While this book and the accompanying CD together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

One key methodology used in this book is to help you discover the exam topics and tools that you need to review in more depth. Remember that the CEH exam will not only expect you to understand hacking concepts but also common tools. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics and when specific tools should be used. This book will help you pass the CEH exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD

Who Should Read This Book?

This book is not designed to be a general security book or one that teaches network defenses. This book looks specifically at how attackers target networks, what tools attackers use, and how these techniques can be used by ethical hackers. Overall, this book is written with one goal in mind: to help you pass the exam.

So, why should you want to pass the CEH exam? Because it's one of the leading entry-level hacking certifications. It is also featured as part of DoD 8570, and having the certification might mean a raise, a promotion, or other recognition. It's also a chance to enhance your resumé and to demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. Or one of many other reasons.

Strategies for Exam Preparation

Although this book is designed to prepare you to take and pass the CEH certification exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exam and additional exams provided in the test software. Your results should tell you whether you are ready for the real thing.

When taking the actual certification exam, make sure that you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best as you can, and then mark it for review.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the CEH certification are designed to ensure that you have that solid foundation.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about scanning and Nmap if you fully understand the tool already. However, many people like to make sure that they truly know a topic and therefore read over material that they already know. Several book features will help you gain the confidence that you need to be convinced that you know some material already, and to also help you know what topics you need to study more.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. Chapter 1 provides an overview of ethical hacking and reviews some basics. Chapters 2 through 13 are the core chapters. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 2 through 13, cover the following topics:

- **Chapter 2, "The Technical Foundations of Hacking"**—This chapter discusses basic techniques that every security professional should know. This chapter reviews TCP/IP and essential network knowledge.
- **Chapter 3, "Footprinting and Scanning"**—This chapter discusses the basic ideas behind target selection and footprinting. The chapter reviews what type of information should be researched during footprinting and how passive and active footprinting and scanning tools should be used.
- **Chapter 4, "Enumeration and System Hacking"**—This chapter covers enumeration, and it is a final chance to uncover more detailed information about a target before system hacking. System hacking introduces the first step at which the hacker is actually exploiting a vulnerability systems.
- **Chapter 5, "Linux and Automated Assessment Tools"**—This chapter examines the role of Linux in the hacking community and how Linux distributions such as Backtrack are used. This chapter also reviews automated security tools such as Metasploit and Canvas.

- **Chapter 6, "Trojans and Backdoors"**—This chapter covers the ways in which Trojans and backdoors function. It reviews the methods in which the tools are deployed and used.
- **Chapter 7, "Sniffers, Session Hijacking, and Denial of Service"**—This chapter covers sniffing tools such as Wireshark. The chapter examines the difference in passive and active sniffing. It also reviews session hijacking and DoS, DDoS, and botnet techniques.
- **Chapter 8, "Web Server Hacking, Web Applications, and Database Attacks"**—This chapter covers the basics of web hacking, application attacks, and how SQL injection works.
- **Chapter 9, "Wireless Technologies, Mobile Security, and Attacks"**—This chapter examines the underlying technology of wireless technologies, mobile devices, Android, IOS, and Bluetooth.
- **Chapter 10, "IDS, Firewalls, and Honeypots"**—This chapter discusses how attackers bypass intrusion detection systems and firewalls. This chapter also reviews honeypots and honeynets and how they are used to jail attackers.
- **Chapter 11, "Buffer Overflows, Viruses, and Worms"**—This chapter covers the fundamentals of buffer overflows. The chapter also examines basic types of malware such as viruses and worms, and examines static and active analysis of malicious code.
- **Chapter 12, "Cryptographic Attacks and Defenses"**—This chapter covers the fundamentals of attacking cryptographic systems and how tools such as encryption can be used to protect critical assets.
- **Chapter 13, "Physical Security and Social Engineering"**—This chapter covers the fundamentals of social engineering attacks and introduces the concept that not all attacks are technical in nature. Attacks can be technical, social, or even physical. Finally, this chapter reviews important concepts of penetration testing.

This page intentionally left blank

This page intentionally left blank

This chapter covers the following topics:

- **Enumeration:** The process of counting off or listing what services, applications, and protocols are present on each identified computer.
- **System Hacking:** The process of gaining access, escalating privileges, maintaining control, and covering tracks.

CHAPTER 4

Enumeration and System Hacking

This chapter introduces Windows enumeration and system hacking. It gives you the knowledge you need to prepare for the Certified Ethical Hacker exam, and it broadens your knowledge of Windows security controls and weaknesses. However, this chapter addresses only the basic information, as it would require an entire book to cover all Windows hacking issues. If you are seriously considering a career as a penetration tester, this chapter should whet your appetite for greater knowledge.

The chapter begins by introducing enumeration and discusses what kind of information can potentially be uncovered. Enumeration is the final pre-attack phase in which you probe for usernames, system roles, account details, open shares, and weak passwords. This chapter also reviews some basics of Windows architecture. A review of Windows users and groups is discussed. The last topic is system hacking. This section discusses the tools and techniques used for gaining access to computer systems. Although many of the tools introduced are specific to Windows systems, the steps are the same no matter what the platform, as evident in Chapter5, "Linux and Automated Assessment Tools," when Linux is discussed.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 4-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Enumeration	2, 3, 4, 5, 10
System Hacking	1, 6, 7, 8, 9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is considered a nontechnical attack?
   a. Password sniffing
   b. Dumpster diving
   c. Password injection
   d. Software keylogger

2. A RID of 500 is associated with what account?
   a. A user account
   b. The first users account
   c. The guest account
   d. The administrator account

3. During enumeration what ports may specifically indicate SMB on a Windows computer?
   a. 110
   b. 111
   c. 389
   d. 445

4. During enumeration what ports may specifically indicate portmapper on a Linux computer?
   a. 110
   b. 111
   c. 389
   d. 445

5. Which of the following is a tool commonly used for enumeration?
   a. GetAcct
   b. John

c. LCP
d. IAM tool kit

6. Which type of password cracking makes use of the space/time memory trade-off?
   a. Dictionary attack
   b. Rainbow table
   c. Rule
   d. Hybrid

7. The second layer of security on the SAM file is known as what?
   a. Encoding
   b. Obscuring
   c. SYSKEY
   d. Salting

8. Windows passwords that are stored in seven-character fields are known as what?
   a. NTLMv2
   b. Kerberos
   c. Salted
   d. LAN Manager

9. Which of the following matches the common padding found on the end of short Windows passwords?
   a. 1404EE
   b. EE4403
   c. EEEEEE
   d. 1902DD

10. If you were going to enumerate DNS, which of the following tools could be used?
    a. Route print
    b. ARP -A
    c. Nslookup
    d. IPconfig

Foundation Topics

Key Topic

Enumeration

Enumeration can be described as an in-depth analysis of targeted computers. Enumeration is performed by actively connecting to each system to identify the user accounts, system accounts, services, and other system details. Enumeration is the process of actively querying or connecting to a target system to acquire information on: NetBIOS/LDAP, SNMP, UNIX/Linux operation, NTP servers, SMTP servers, and DNS servers. These topics are discussed next.

Windows Enumeration

The object of Windows enumeration is to identify a user account or system account for potential use. You might not have to find a system administrator account because escalation of privilege may be possible. At this point, we are simply seeking the knowledge to gain some level of access.

To better target Microsoft Windows computers, you should understand how they function. Windows ships with both client and server versions. Client systems that are still being supported as of this writing include the following: Windows XP, Vista, 7, and 8. On the server side, Microsoft supports Windows 2003, 2008, and 2012. Each of these operating systems shares a somewhat similar kernel. The kernel is the most trusted part of the operating system. How does the operating system know who and what to trust? The answer is by implementing rings of protection. The protection ring model provides the operating system with various levels at which to execute code or restrict its access. It provides a level of access control and granularity. As you move toward the outer bounds of the model, the numbers increase, and the level of trust decrease. Figure 4-1 shows the basic model that Windows uses for protective rings.

With the Windows architecture, you can see that there are two basic modes: user mode (ring 3) and kernel mode (ring 0). User mode has restrictions, whereas kernel mode allows full access to all resources. This is an important concept for the ethical hacker to contemplate because antivirus and analysis tools can detect hacking tools and code that run in user mode. However, if code can be deployed on a Windows system to run in kernel mode, it can hide itself from user mode detection and will be harder to detect and eradicate. All the code that runs on a Windows computer must run in the context of an account. The system account has the capability to perform kernel mode activities. The level of the account you hold determines your ability to execute code on a system. Hackers always want to run code at the highest possible privilege. Windows uses the following two things to help keep track of a user's security rights and identity:

- Security identifiers (SIDs)
- Relative identifiers (RIDs)

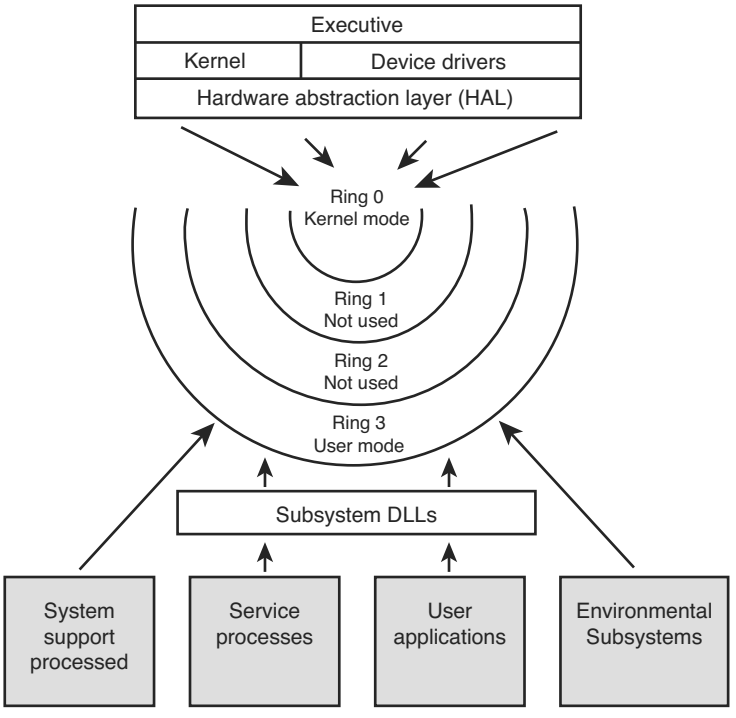

Figure 4-1 Windows architecture.

SIDs are a data structure of variable length that identifies user, group, and computer accounts. For example, a SID of S-1-1-0 indicates a group that includes all users. Closely tied to SIDs are RIDs. A RID is a portion of the SID that identifies a user or group in relation to the authority that user has. Let's look at an example:

```
S-1-5-21-1607980848-492894223-1202660629-500
     S for security id
     1 Revision level
     5 Identifier Authority (48 bit) 5 = logon id
     21 Sub-authority (21 = nt non unique)
     1607980848       SA
     492894223        SA domain id
     1202660629       SA
     500               User  id
```

Focus your attention on the last line of text in this example. The user ID specifies the specific user, as shown in Table 4-2.

Key Topic

Table 4-2 User ID and Corresponding RID Code

User ID	Code
Admin	500
Guest	501
Kerberos	502
First user	1000
Second user	1001

This table shows that the administrator account has a RID of 500 by default, the guest has a RID 501, and the first user account has a RID of 1000. Each new user gets the next available RID. This information is important because simply renaming an account will not prevent someone from discovering key accounts. This is similar to the way that Linux controls access for users and system processes through an assigned user ID (UID) and a group ID (GID) that is found in the /etc/passwd file. On a related topic, let's look at some other important security components of Microsoft Windows that will help you understand the enumeration process.

TIP Be able to correlate specific user accounts and RIDs for the exam, such as 501 = guest.

Windows Security

On a standalone Windows computer, user information and passwords are stored in the Security Account Manager (SAM) database. If the system is part of a domain, the domain controller stores the critical information in Active Directory (AD). On standalone systems not functioning as domain controllers, SAM contains the defined local users and groups, along with their passwords and other attributes. The SAM database is stored in Windows/System32/config folder in a protected area of the Registry under HKLM\SAM.

AD is a directory service, which contains a database that stores information about objects in a domain. AD keeps password information and privileges for domain users and groups that were once kept in the domain SAM. Unlike the old NT trust model, a domain is a collection of computers and their associated security groups

that are managed as a single entity. AD was designed to be compatible to Lightweight Directory Access Protocol (LDAP); you can get more background information from RFC 2251.

Another important Windows security mechanism is Local security authority subsystem (Lsass). It might sound familiar to you: Lsass is what the Sasser worm exploited by buffer overflow in 2004. Lsass is a user mode process that is responsible for the local system security policy. This includes controlling access, managing password policies, user authentication, and sending security audit messages to the event log.

NetBIOS and LDAP Enumeration

NetBIOS was a creation of IBM. It is considered a legacy protocol today but may still be found on some older systems. On local-area networks (LANs), NetBIOS systems usually identify themselves by using a 15-character unique name. Because NetBIOS is nonroutable by default, Microsoft adapted it to run over Transmission Control Protocol/Internet Protocol (TCP/IP). NetBIOS is used in conjunction with Server Message Blocks (SMBs). SMB allows for the remote access of shared directories and files. These services are provided through the ports shown in Table 4-3.

Table 4-3 Microsoft Key Ports and Protocols

Key Topic

Port	Protocol	Service
135	TCP	MS-RPC endpoint mapper
137	UDP	NetBIOS name service
138	UDP	NetBIOS datagram service
139	TCP	NetBIOS session service
445	TCP	SMB over TCP

This table lists key ports and protocols that Microsoft systems use. When performing a port scan or attempting to identify a system, finding these open ports will signal that you might be dealing with a Microsoft system. After these ports have been identified, you can begin to further enumerate each system.

TIP Make sure that you can identify key Windows ports.

SMB was designed to make it possible for users to share files and folders, although InterProcess Communication (IPC) offers a default share on Windows systems.

This share, the IPC$, was used to support named pipes that programs use for interprocess (or process-to-process) communications. Because named pipes can be redirected over the network to connect local and remote systems, they also enable remote administration. As you might think, this can be a problem.

A null session occurs when you log in to a system with no user ID and password at all. In legacy Windows versions 2000, XP, and Windows 2003, a null session could be set up using the `net` command.

There's an entire host of `net` commands. A few are discussed here, but for a more complete list, just type **net** from the command line and the **/?** syntax after any of the commands you see that you would like more information on.

Even though you may not see the IPC$ share when looking for shared drives and folders, that doesn't mean that it is not there. For example, if you have identified open ports of 135, 139, and 445 on some targeted systems, you might attempt the `net view /domain` command:

```
C:\>net view /domain
Domain
SALES
MARKETING
ACCOUNTING
The command completed successfully.
```

Notice that these `net` commands are quite handy. They have identified the sales, marketing, and accounting groups. To query any specific domain group, just use the net command again in the form of `net view /domain:`*`domain_name`*:

```
C:\>net view /domain:accounting
Server Name             Remark
\\Mickey
\\Pluto
\\Donald
The command completed successfully.
```

You can take a closer look at any one system by using the `net view \ \`*`system_name`* command:

```
C:\net view \\donald
Shared resources at \\DONALD
Sharename     Type          Comment
-------------------------------------------------------
CDRW          Disk
D             Disk
Payroll       Disk
```

```
Printer       Disk
Temp          Disk
The command was completed successfully.
```

Now that you have completed some basic groundwork, let's move on to enumerating user details, account information, weak passwords, and so on. `IPC$` is further exploited for these activities. Specifically, you will need to set up a null session. You can do so manually with the `net` command:

```
C:\net use \\donald\ipc$ "" /u:""
```

NOTE Setting up a null session to take advantage of Windows underlying communication protocols has been secured with newer operating systems such as Server 2012, Windows 7, and Windows 8, but you might still find a few old systems on which this is possible.

NetBIOS Enumeration Tools

With a `net use \\` *`computer name`*`\ ipc$ "" /u:""` command executed, you're primed to start hacking at the system. The tools discussed in this section, such DumpSec and GetAcct, require that you have a null session established before you attempt to use them.

DumpSec is a Windows-based graphical user interface (GUI) enumeration tool from SomarSoft. It enables you to remotely connect to Windows machines and dump account details, share permissions, and user information. It is shown in Figure 4-2. Its GUI-based format makes it easy to take the results and port them into a spreadsheet so that holes in system security are readily apparent and easily tracked. It can provide you with usernames, SIDs, RIDs, account comments, account policies, and dial-in information.

GetAcct enables you to input the IP address or NetBIOS name of a target computer and extract account information. It can extract SID, RID, comments, full name, and so on. From our discussion earlier about SIDs on Windows machines, you know that the administrator account on the machine ends in 500. Therefore, you can use GetAcct to discover the SID for the usernames found in your enumeration and discover who has administrative access.

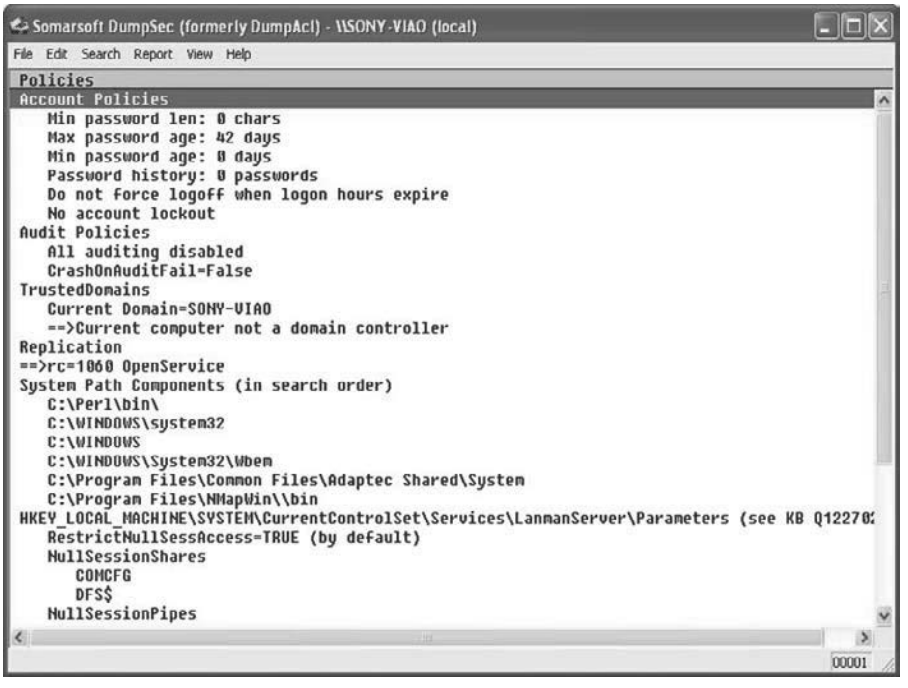

Figure 4-2 DumpSec.

Many tools can be used for enumeration. The ones listed here should give you an idea of what this category of tool can do. Listed here are some other tools that perform the same type of enumeration:

- **SuperScan:** Released by Foundstone, SuperScan retrieves all available information about any known user from any vulnerable Windows system.
- **GetUserInfo:** Created by JoeWare, this command-line tool extracts user info from a domain or computer.
- **Ldp:** This executable is what you need if you're working with AD systems. After you find port 389 open and authenticate yourself using an account (even guest will work), you will be able to enumerate all the users and built-in groups.
- **User2sid:** This program can retrieve a SID from the SAM from the local or a remote machine. Sid2user.exe can then be used to retrieve the names of all the user accounts and more. For example, typing `user2sid \\ computer name` returns the name and corresponding SID.

Other tools are available to enumerate a Windows system. For example, if you are local to the system, you can also use NBTStat. Microsoft defines NBTStat as a tool

designed to help troubleshoot NetBIOS name resolution problems. It has options such as local cache lookup, WINS server query, broadcast, LMHOSTS lookup, Hosts lookup, and DNS server query. Typing **nbtstat** at a Windows command prompt will tell you all about its usage:

```
C:\ nbtstat
Displays protocol statistics and current TCP/IP connections using
NBT(NetBIOS over TCP/IP).
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n]
         [-r] [-R] [-s] [S] [interval] ]
```

One of the best ways to use NBTstat is with the `-A` option. Let's look at what that returns:

```
C:\ >NBTstat -A 192.168.13.10

            NetBIOS Remote Machine Name Table

       Name                 Type          Status
    ---------------------------------------------
    DONALD          <00>    UNIQUE        Registered
    WORKGROUP       <00>    GROUP         Registered
    DONALD          <20>    UNIQUE        Registered
    WORKGROUP       <1E>    GROUP         Registered
    WORKGROUP       <1D>    UNIQUE        Registered
    ..__MSBROWSE__. <01>    GROUP         Registered

    MAC Address = 00-19-5D-1F-26-68
```

A name table that provides specific hex codes and tags of unique or group is returned. These codes identify the services running on this specific system. For example, do you see the code of `1D UNIQUE`? This signifies that the system Donald is the master browser for this particular workgroup. Other common codes include the following:

Title	Hex Value	User/Group	Service
domain	1B	U	Domain master browser
domain	1C	G	Domain controllers
domain	1D	U	Master browser
domain	1E	G	Browser service elections

You can find a complete list of NetBIOS name codes at www.cotse.com/nbcodes.htm or by searching for NetBIOS name codes.

SNMP Enumeration

Simple Network Management Protocol (SNMP) is a popular TCP/IP standard for remote monitoring and management of hosts, routers, and other nodes and devices on a network. It works through a system of agents and nodes. SNMP is designed so that requests are sent to agents, and the agents send back replies. The requests and replies refer to configuration variables accessible by agent software. Traps are used to signify an event, such as a reboot or interface failure. SNMP makes use of the Management Information Base (MIB). The MIB is the database of configuration variables that resides on the networking device.

SNMP version 3 offers data encryption and authentication, but version 1 and 2 are still in use. Both version 1 and 2 are clear-text protocols that provides only weak security through the use of community strings. The default community strings are public and private and are transmitted in clear text. If the community strings have not been changed or if someone can sniff the community strings, that person then has more than enough to enumerate the vulnerable devices.

NOTE SNMP version 1 and 2 use default community strings of public and private.

Devices that are SNMP enabled share a lot of information about each device that probably should not be shared with unauthorized parties. SNMP enumeration tools can be found in both Windows and Linux. Several are mentioned here:

- **snmpwalk:** A Linux command-line SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.
- **IP Network Browser:** A GUI-based network discovery tool from www.solarwinds.net that enables you to perform a detailed discovery on one device or an entire subnet.
- **SNScan:** A free GUI-based SNMP scanner from Foundstone, shown in Figure 4-3.

The best defense against SNMP enumeration is to turn it off if it is not needed. If it is required, make sure that you block ports 161 and 162 at network chokepoints, and ensure that an upgrade to SNMPv3 is possible. Changing the community strings is another defensive tactic as is making them different in each zone of the network.

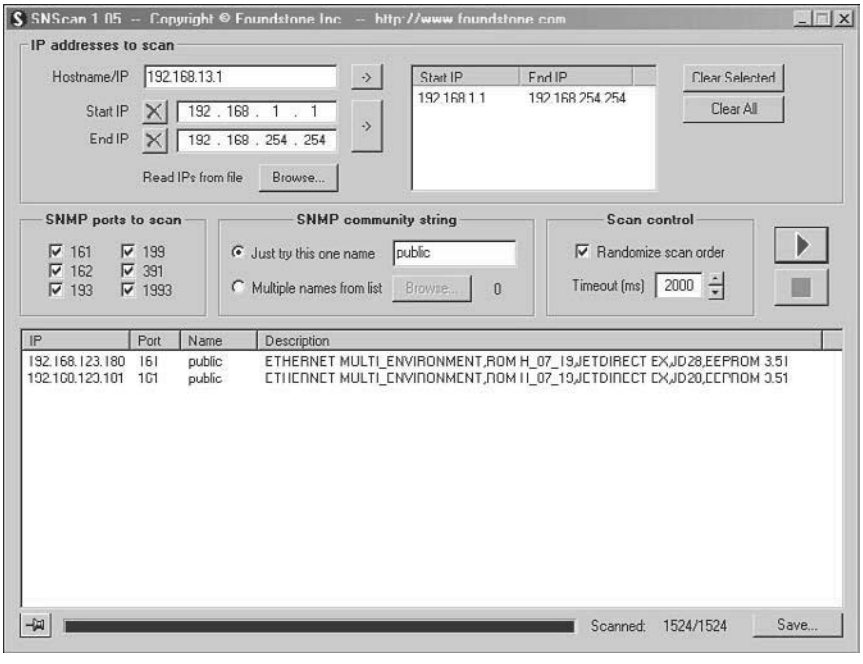

Figure 4-3 SNScan.

Linux/UNIX Enumeration

Even though Linux might not offer the opportunities that Windows systems do, there are still some enumeration techniques you can perform. Tools such as rpcclient can be used to enumerate usernames on those operating systems just like on a Windows system. Some other tools are shown here:

- **Rpcclient:** Using the `rpcclient` command, the attacker can enumerate usernames (for example, `rpcclinet $> netshareenum`).
- **Showmount:** The `showmount` command displays a list of all clients that have remotely mounted a file system from a specified machine in the host parameter.
- **Finger:** The `finger` command enumerates the user and the host. It enables the attacker to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail.
- **Rpfinfo:** The `rpfinfo` command helps to enumerate Remote Procedure Call (RPC) protocol. It makes an RPC call to an RPC server and reports what it finds.

- **Enum4linux:** The `enum4linux` command is used for enumerating information from Windows and Samba systems. The application basically acts as a wrapper around the Samba commands `smbclient`, `rpclient`, `net`, and `nmblookup`.

NTP Enumeration

Network Time Protocol (NTP) is a protocol designed to synchronize clocks of networked computers. Networks using Kerberos or other time-based services need a time server to synchronize systems. NTP uses UDP port 123. Basic commands that can be attempted include the following:

- **Ntpdate:** Used to collect time samples
- **Ntptrace:** Follows time servers back up the chain to primary time server
- **Ntpdc:** Used to query about the state of the time server
- **Ntpq:** Used to monitor performance

NTP enumeration tools include the following:

- PresenTense Time Server
- NTP Server Scanner
- LAN Time Analyzer

SMTP Enumeration

Simple Mail Transfer Protocol (SMTP) is used for the transmission of email messages. SMTP operates on TCP port 25. SMTP is something that a hacker will be interested in because it can potentially be used to perform username enumeration via the `EXPN`, `RCPT`, and `VRFY` commands. Penetration testers can also leverage the usernames that have been obtained from this enumeration to conduct further attacks on other systems. SMTP enumeration can be performed with utilities like Netcat. From the command line, you type the following:

```
nc -v -z -w 2 IP Address 1-1024
```

Other common SMTP enumeration tools include the following:

- NetScan Tools Pro
- Nmap
- Telnet

DNS Enumeration

Domain Name System (DNS) enumeration is the process of locating all information about DNS. This can include identifying internal and external DNS servers and performing lookups of DNS records for information such as usernames, computer names, and IP addresses of potential target systems and performing zone transfers. Much of this activity was done in Chapter 3, "Footprinting and Scanning." The most straightforward way is to use Nslookup, but you can also use other tools. Tools for enumeration include the following:

- DigDug
- WhereIsIP
- NetInspector
- Men and Mice Management Console

System Hacking

Key Topic

System hacking is a big step in the fact that you are no longer simply scanning and enumerating a system. At this point, you are attempting to gain access. Things start to change because this stage is about breaking and entering into the targeted system. Previous steps, such as footprinting, scanning, and enumeration, are all considered pre-attack stages. As stated, before you begin, make sure that you have permission to perform these activities on other people's systems.

The primary goal of the system hacking stage is to authenticate to the remote host with the highest level of access. This section covers some common nontechnical and technical password attacks against authentication systems.

Nontechnical Password Attacks

Attackers are always looking for easy ways to gain access to systems. Hacking authentication systems is getting harder because most organizations have upped their game, using strong authentication and improving auditing controls. That is one reason why nontechnical attacks remain so popular. Basic techniques include the following:

- **Dumpster diving:** Dumpster diving is the act of looking through a company's trash to find information that may help in an attack. Access codes, notes, passwords, and even account information can be found.
- **Social engineering:** We spend much more time discussing social engineering later in the book, but for now what is important to know is that social engineering is the manipulation of people into performing actions or divulging confidential information.

- **Shoulder surfing:** The act of watching over someone's shoulder to get information such as passwords, logins, and account details.

Technical Password Attacks

Technical password attacks require some use of technology. These attacks also build on the information you have obtained in the previous steps. Tools used during enumeration, such as Getacct, IP Network Browser, and net view, may have returned some valuable clues about specific accounts. By now, you may even have account names, know who is the administrator, know whether there is a lockout policy, and even know the names of open shares. Technical password attack techniques discussed here include the following:

- Password guessing
- Automated password guessing
- Password sniffing
- Keyloggers

Many of today's most successful attacks involve both technical and nontechnical elements.

Password Guessing

Guessing usernames and passwords requires that you review your findings. Remember that good documentation is always needed during a penetration test, so make sure that you have recorded all your previous activities. When password guessing is successful, it is usually because people like to use easy to remember words and phrases. A diligent penetration tester or attacker will look for subtle clues throughout the enumeration process to key in on—probably words or phrases the account holder might have used for a password. What do you know about this individual, what are his hobbies? If the account holder is not known to you, focus on accounts that

- Haven't had password changes for a long time
- Have weakly protected service accounts
- Have poorly shared accounts
- Indicate the user has never logged in
- Have information in the comment field that might be used to compromise password security

If you can identify such an account, you can issue the `net use` command from the command line to attempt the connection:

```
net use * \\IP_address\share * /u:name
```

You'll be prompted for a password to complete the authentication:

```
C:\ >net use * \\192.188.13.10\c$ * /u:jack
Type the password for \\172.20.10.79\c$:
The command completed successfully
```

Automated Password Guessing

Because you may want to set up a method of trying each account once or twice for weak passwords, you might consider looping the process. Automated password guessing can be performed by constructing a simple loop using the Windows command shell. It is based on the standard `net use` syntax. The steps are as follows:

1. Create a simple username and password file.
2. Pipe this file into a `FOR` command as follows:

```
C:\ > FOR  /F "token=1, 2*" %i in (credentials.txt) do net use \\target\IPC$
        %i /u:%j
```

Many dedicated software programs automate password guessing. Some of the more popular free tools include NAT, Brutus, THC Hydra, and Venom. NetBIOS Auditing Tool (NAT) is a command-line automated password guessing tool. Just build a valid list of users from the tools discussed during enumeration. Save the usernames to a text file. Now create a second list with potential passwords. Feed both of these into NAT, as follows:

```
nat [-o filename] [-u userlist] [-p passlist] <address>
```

NAT attempts to use each name to authenticate with each password. If it is successful, it halts the program at that point. Then you want to remove that name and start again to find any additional matches. You can grab a copy of NAT at www.tux.org/pub/security/secnet/tools/nat10/.

NOTE Make sure that you identify whether there is a password lockout policy, because you might have only two or three tries before the account is locked. Otherwise, you might inadvertently cause a denial of service (DoS) if you lock out all the users.

Password Sniffing

If your attempts to guess passwords have not been successful, sniffing or keystroke loggers might offer hope. Do you ever think about how much traffic passes over a typical network every day? Most networks handle a ton of traffic, and a large portion of it might not even be encrypted. Password sniffing requires that you have physical or logical access to the device. If that can be achieved, you can simply sniff the credentials right off the wire as users log in.

One such tool is Pass-The-Hash. This application allows an attacker to authenticate to a remote server using the LM/NTLM hash of a user's password, eliminating the need to crack/brute-force the hashes to obtain the clear-text password. Because Windows does not salt passwords, they remain static from session to session until the password is changed. If an attacker can obtain a password hash, it can be functionally equivalent to obtaining the clear-text password. Rather than attempting to crack the hash, attackers can simply replay them to gain unauthorized access. You can download Pass-The-Hash at http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=Pass-The-Hash_Toolkit. ScoopLM is another tool designed to sniff password hashes; it sniffs for Windows authentication traffic. When passwords are detected and captured, it features a built-in dictionary and brute-force cracker.

Besides capturing Windows authentications, there are also tools to capture and crack Kerberos authentication. Remember that the Kerberos protocol was developed to provide a secure means for mutual authentication between a client and a server. It enables the organization to implement single sign-on (SSO). You should already have a good idea if Kerberos is being used, as you most likely scanned port 88, the default port for Kerberos, in an earlier step.

KerbCrack, a tool from NTSecurity.nu, can be used to attack Kerberos. It consists of two separate programs. The first portion is a sniffer that listens on port 88 for Kerberos logins, and the second portion is used as a cracking program to dictionary or brute-force the password. If all this talk of sniffing has raised your interest in the topic, you'll enjoy Chapter 7, "Sniffers, Session Hijacking, and Denial of Service," which covers sniffers in detail.

TIP If none of the options discussed previously are feasible, there is still keystroke logging, which is discussed next.

Keystroke Loggers

Keystroke loggers can be software or hardware devices used to monitor activity. Although an outsider to a company might have some trouble getting one of these devices installed, an insider is in a prime position.

Hardware keystroke loggers are usually installed while users are away from their desks and are completely undetectable, except for their physical presence. When was the last time you looked at the back of your computer? Even then, they can be overlooked because they resemble a keyboard extension cable or adapter; www.keyghost.com has a large collection. Some hardware keyloggers use WiFi, which means that once it is deployed the attacker does not have to retrieve the device and can communicate with it remotely via wireless or Bluetooth connection.

Software keystroke loggers sit between the operating system and the keyboard. Most of these software programs are simple, but some are more complex and can even email the logged keystrokes back to a preconfigured address. What they all have in common is that they operate in stealth mode and can grab all the text a user enters. Table 4-4 shows some common keystroke loggers.

Table 4-4 Software Keystroke Loggers

Product	URL
ISpyNow	www.ispynow.net
PC Activity Monitor	PCActivityMonitor.org
RemoteSpy	www.remotespy.com
Spector	www.spectorsoft.com
KeyStrokeSpy	www.keylogger-software.com

TIP Keystroke loggers are one way to obtain usernames and passwords.

Privilege Escalation and Exploiting Vulnerabilities

If the attacker can gain access to a Windows system as a standard user, the next step is privilege escalation. This step is required because standard user accounts are limited; to be in full control, administrator access is needed. This might not always be an easy task because privilege-escalation tools must be executed on the victim's

system. How do you get the victim to help you exploit a vulnerability? Common techniques include the following:

- Exploiting an application
- Tricking the user into executing the program
- Copying the privilege escalation tool to the targeted system and schedule the exploit to run at a predetermined time, such as the `AT` command
- Gaining interactive access to the system, such as Terminal Server, pcAnywhere, and so on

Exploiting an Application

Sometimes a hacker can get lucky and exploit a built-in application. For example, when you press the Shift key five or more times Windows opens StickyKeys options for you. The resulting dialog box that appears is an interface to enable the use of StickyKeys, which is a Windows feature to aid handicapped users. There is nothing wrong with the use of this feature. The only problem is how it is implemented. If an attacker can gain access, it mght be possible to replace sethc.exe with cmd.exe. After replacing the file, you can invoke the command prompt and execute explorer.exe and commands with full access to the computer.

The reason this attacks works is because it slips through all of Windows protection checks. Windows first checks whether the .exe is digitally signed, which cmd.exe is. Next, it checks that the .exe is located in the system directory (%systemroot%\system32), thus validating integrity level and administrator permissions. Windows then checks to make sure the executable is on its internal list of Windows protected system files and known to be part of the OS, which cmd.exe is and therefore passes. Therefore, Windows thinks that it is launching the accessibility feature StickyKeys, but instead it is launching shellcode running as LocalSystem.

Exploiting a Buffer Overflow

It's important to realize that buffer overflows, memory corruption, heap attacks are patched over time. Therefore, these exploits work only for specific versions of operating system or application. An example of this can be seen with the Aurora exploit. This exploit was used to gain access on vulnerable Windows systems running Internet Explorer 6. The exploit caused a memory corruption flaw in Internet Explorer. This flaw was found in the wild and was a key component of the Operation Aurora attacks used against Google and others. The attack works by spraying the heap with a large amount of data. Heap spraying is the act of loading a large amount of data in the heap along with some shellcode. The aim of placing all of this data onto the

heap is to create the right conditions in memory to allow the shellcode to be executed.

Java is another application that has been exploited in several attacks. One example is the Java watering hole attacks in 2013. Stack-based buffer overflows in the Java Stored Procedure infrastructure allows remotely authenticated users to execute arbitrary code by leveraging certain CONNECT and EXECUTE privileges. Some well-known privilege-escalation tools are shown here:

- **Billybastard.c:** Windows 2003 and XP
- **ANI Exploit:** Windows Vista
- **Getad.exe:** Windows 2003 and XP
- **ERunAs2X.exe:** Windows 2000

TIP Keeping systems and applications patched is one of the best countermeasures you can do to defend against privilege-escalation tools.

Owning the Box

One of the first activities an attacker wants to do after he owns the box is to make sure that he has continued access and that he has attempted to cover his tracks. One way to ensure continued access is to compromise other accounts. Stealing SAM is going to give the attacker potential access to all the passwords. SAM contains the user account passwords stored in their hashed form. Microsoft raised the bar with the release of NT Service Pack 3 by adding a second layer of encryption called SYSKEY. SYSKEY adds a second layer of 128-bit encryption. After being enabled, this key is required by the system every time it is started so that the password data is accessible for authentication purposes.

Attackers can steal the SAM through physical or logical access. If physical access is possible, the SAM can be obtained from the NT ERD (Emergency Repair Disk) from C:\winnt\repair\sam. Newer versions of Windows place a backup copy in C:\winnt\repair\regback\sam, although SYSKEY prevents this from easily being cracked. One final note here is that you can always just reset the passwords. If you have physical access, you can simply use tools such as LINNT and NTFSDOS to gain access. NTFSDOS can mount any NTFS partition as a logical drive. NTFSDOS is a read-only network file system driver for DOS/Windows. If loaded onto a CD or thumb drive, it makes a powerful access tool. Logical access presents some easier possibilities. The Windows SAM database is a binary format, so it's not

easy to directly inspect. Tools such as PWdump and LCP can be used to extract and crack SAM. Before those programs are examined, let's briefly review how Windows encrypts passwords and authenticates users.

Authentication Types

Windows supports many authentication protocols, including those used for network authentication, dialup authentication, and Internet authentication. For network authentication and local users, Windows supports Windows NT Challenge/Response, also known as NTLM. Windows authentication algorithms have improved over time. The original LAN Manager (LM) authentication has been replaced by NTLMv2. Windows authentication protocols include the following:

- **LM authentication:** Used by 95/98/Me and is based on DES
- **NTLM authentication:** Used by NT until Service Pack 3 and is based on DES and MD4
- **NTLM v2 authentication:** Used post-NT Service Pack 3 and is based on MD4 and MD5
- **Kerberos:** Implemented first in Windows 2000 and can be used by all current versions of Windows, including Server 2012 and Windows 8

Because of backward compatibility, LM can still be used. These encrypted passwords are particularly easy to crack because an LM password is uppercased, padded to 14 characters, and divided into two 7-character parts. The two hashed results are concatenated and stored as the LM hash, which is stored in SAM. To see how weak this system is, consider the following example. Let's say that an LM password to be encrypted is Dilbert!:

1. When this password is encrypted with an LM algorithm, it is converted to all uppercase: DILBERT!
2. Then the password is padded with null (blank) characters to make it a 14-character length: DILBERT!_ _ _ _ _ _
3. Before encrypting this password, the 14-character string is divided into two seven character pieces: DILBERT and !_ _ _ _ _ _
4. Each string is encrypted individually, and the results are concatenated together.

With the knowledge of how LM passwords are created, examine the two following password entries that have been extracted from SAM with PWdump:

```
Bart:  1001:
B79135112A43EC2AAD3B431404EE:
DEAC47322ABERTE67D9C08A7958A:

Homer: 1002:
B83A4FB0461F70A3B435B51404EE:
GFAWERTB7FFE33E43A2402D8DA37:
```

Notice how each entry has been extracted in two separate character fields? Can you see how the first half of each portion of the hash ends with 1404EE? That is the padding, and this is how password-cracking programs know the length of the LM password. It also aids in password-cracking time. Just consider the original Dilbert! example. If extracted, one seven-character field will hold Dilbert, whereas the other only has one character (!).

Cracking 1 character or even 7 is much easier than cracking a full 14. Fortunately, Windows has moved on to more secure password algorithms. Windows can use six levels of authentication now, as shown in Table 4-5. Using longer passwords, greater than 14 characters, and using stronger algorithms is one of the best defenses against cracking passwords.

Table 4-5 LM, NTLM, and NTLM2

Attribute	LM	NTLM	NTLMv2
Password	Yes	No	No
Hash	DES	MD4	MD5
Algorithm	DES	DES	HMAC

TIP Kerberos authentication started with Windows 2000 and is the default authentication on all current versions of Microsoft Windows products. Kerberos is considered a strong form of authentication.

Cracking the Passwords

One direct way to remove the passwords from a local or remote system is by using L0phtcrack. L0phtcrack is a Windows password-cracking tool. LC6 is the current version. It can extract hashes from the local machine, a remote machine, and can sniff passwords from the local network if you have administrative rights.

Tools like FGdump and PWdump are other good password-extraction tools. You can get a copy of this tool at www.openwall.com/passwords/nt.shtml. This command-line tool can bypass SYSKEY encryption if you have administrative access. PWdump works by a process of dynamic link library (DLL) injection. This allows the program to hijack a privileged process. PWdump7, the current version, was expanded to allow remote access to the victim system. The program is shown here:

```
C:\ pwdump>pwdump7 192.168.13.10 password.txt
Completed.
```

For PWdump7 to work correctly, you need to establish a session to an administrative share. The resulting text file reveals the hashed passwords:

```
C:\ pwdump>type password.txt
Jack:       500:       A34A4329AAD3MFEB435B51404EE:
                       FD02A1237LSS80CC22D98644FE0:
Ben:       1000:       466C097A37B26C0CAA5B51404EE:
                       F2477A14LK4DFF4F2AC3E3207FE0:
Guest:      501:       NO PASSWORD*********************:
                       NO PASSWORD*********************:
Martha:    1001:       D79135112A43EC2AAD3B431404EE:
                       EEAC47322ABERTE67D9C08A7958A:
Curley:    1002:       D83A4FB0461F70A3B435B51404EE:
                       BFAWERTB7FFE33E43A2402D8DA37
```

With the hashed passwords safely stored in the text file, the next step is to perform a password crack. Historically, three basic types of password cracking exist: dictionary, hybrid, and brute-force attacks.

A dictionary password attack pulls words from the dictionary or word lists to attempt to discover a user's password. A dictionary attack uses a predefined dictionary to look for a match between the encrypted password and the encrypted dictionary word. Many times, dictionary attacks will recover a user's password in a short period of time if simple dictionary words are used.

A hybrid attack uses a dictionary or a word list and then prepends and appends characters and numbers to dictionary words in an attempt to crack the user's password. These programs are comparatively smart because they can manipulate a word and use its variations. For example, take the word *password*. A hybrid password audit would attempt variations such as 1password, password1, p@ssword, pa44w0rd, and so on. Hybrid attacks might add some time to the password-cracking process, but they increase the odds of successfully cracking an ordinary word that has had some variation added to it.

A brute-force attack uses random numbers and characters to crack a user's password. A brute-force attack on an encrypted password can take hours, days, months, or years, depending on the complexity and length of the password. The speed of success depends on the speed of the CPU's power. Brute-force audits attempt every combination of letters, numbers, and characters.

Tools such as L0phtcrack, LCP, Cain and Abel, and John the Ripper can all perform dictionary, hybrid, and brute-force password cracking. The most popular are explained in the following list:

- Cain and Abel is a multipurpose tool that can perform a variety of tasks, including password cracking, Windows enumeration, and Voice over IP (VoIP) sniffing. The password-cracking portion of the program can perform dictionary/brute-force attacks and can use precomputed rainbow tables. It is shown in Figure 4-4. Notice the many types of password cracking it can perform.

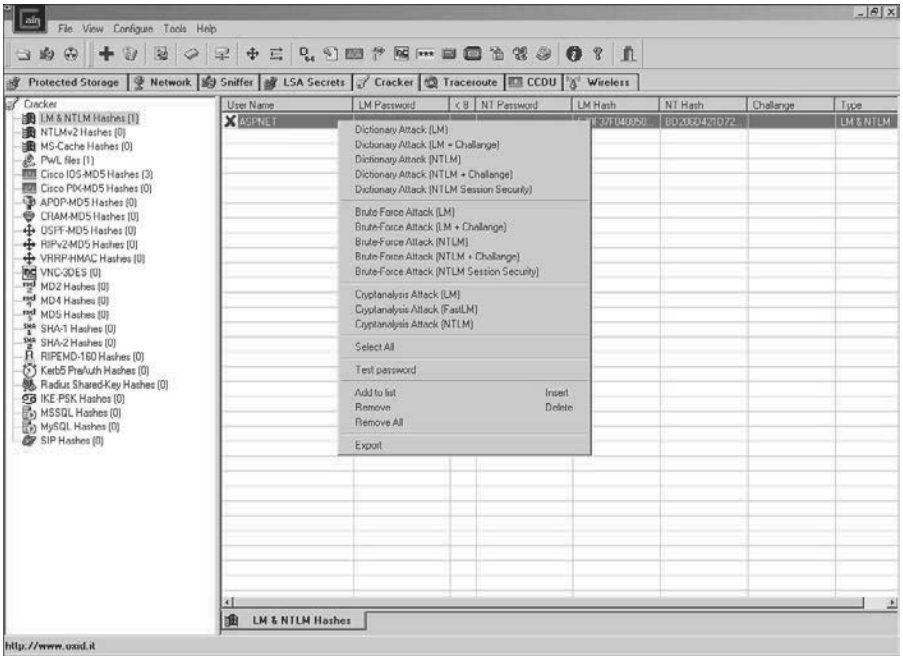

Figure 4-4 Cain and Abel.

- John the Ripper is another great password-auditing tool. It is available for 11 types of UNIX systems, plus Windows. It can crack most common passwords, including Kerberos AFS and Windows hashes. Also, a large number of add-on modules are available for John the Ripper that can enable it to crack OpenVMS passwords, Windows credentials cache, and MySQL passwords. Just

remember that the cracked passwords are not case sensitive and might not represent the real mixed-case password. A determined attacker can overcome this small hindrance.

Years ago, dictionary, hybrid, and brute-force attacks were the primary methods used to recover passwords or attempt to crack them. Many passwords were considered secure just because of the time it would take to crack them. This time factor was what made these passwords seem secure. If given enough time, the password could be cracked, but it might take several months. A relatively new approach to password cracking has changed this belief. It works by means of a rainbow table. The RainbowCrack technique is the implementation of Philippe Oechslin's faster time-memory trade-off technique. It works by precomputing all possible passwords in advance. After this time-consuming process is complete, the passwords and their corresponding encrypted values are stored in a file called a rainbow table. An encrypted password can be quickly compared to the values stored in the table and cracked within a few seconds. RainbowCrack and Ophcrack are examples of two such programs.

Ophcrack is a password-cracking tool that implements the rainbow table techniques previously discussed. What's most important to note here is that if a password is in the rainbow table, it will be cracked quickly. Its website also lets you enter a hash and reveal the password in just a few seconds.

Hiding Files and Covering Tracks

Before moving on to other systems, the attacker must attend to a few unfinished items. According to Locard's exchange principle, "Whenever someone comes in contact with another person, place, or thing, something of that person is left behind." This means that the attacker must disable logging, clear log files, eliminate evidence, plant additional tools, and cover his tracks. Listed here are some of the techniques that an attacker can use to cover his tracks.

- **Disabling logging:** Auditpol was originally included in the NT Resource Kit for administrators. It works well for hackers, too, as long as they have administrative access. Just point it at the victim's system as follows:

```
C:\ >auditpol \\ 192.168.13.10 /disable
Auditing Disabled
```

- **Clear the log file:** The attacker will also attempt to clear the log. Tools such as Winzapper, Evidence Eliminator, and ELSave can be used. ELSave will remove all entries from the logs, except one entry that shows the logs were cleared. It is used as follows:

```
elsave -s \\192.168.13.10 -l "Security" -C
```

One way for attackers to cover their tracks is with rootkits. Rootkits are malicious codes designed to allow an attacker to get expanded access and hide his presence. Rootkits were traditionally a Linux tool, but they are now starting to make their way into the Windows environment. Rootkits such as FU, Vanquish, Hacker Defender, and AFX are all available for Windows systems.

Rootkits can be classified as hypervisor, kernel level, application level, hardware/firmware, boot loader, and library level. Some of these rootkits, such as kernel level, are particularly dangerous because they take control of the operating system kernel. If you suspect that a computer has been rootkitted, you need to use an MD5 hashing utility or a program, such as Tripwire, to determine the viability of your programs. The only other alternative is to rebuild the computer from known good media.

File Hiding

Various techniques are used by attackers to hide their tools on the compromised computer. Some attackers might just attempt to use the `attribute` command to hide files, whereas others might place their files in low traffic areas. A more advanced method is to use NTFS alternate data streams (ADS). NTFS ADS was developed to provide for compatibility outside of the Windows world with structures, such as the Macintosh Hierarchical File System (HFS). These structures use resource forks to maintain information associated with a file, such as icons and so on.

The streams are a security concern because an attacker can use these streams to hide files on a system. ADS provides hackers with a means of hiding malware or hacking tools on a system to later be executed without being detected by the systems administrator. Because the streams are almost completely hidden, they represent a near-perfect hiding spot on a file system. It allows the attacker the perfect place to hide his tools until he needs to use them at a later date. An ADS stream is essentially files that can be executed. To delete a stream, its pointer must be deleted first (or copy the pointer file to a FAT file system). That will delete the stream because FAT cannot support ADS. To create an ADS, issue the following command:

```
Type certguide.zip > readme.txt:certguide.zip
```

This command streamed certguide.zip behind readme.txt. This is all that is required to stream the file. Now the original secret file can be erased:

```
Erase certguide.zip
```

All the hacker must do to retrieve the hidden file is to type the following:

```
Start c:\readme.txt:certguide.zip
```

This will execute ADS and open the secret file. Tools that can detect streamed files include the following:

- **Streams:** A Microsoft tool
- **Sfind:** A Foundstone forensic tool for finding streamed files
- **LNS:** Another tool used for finding streamed files, developed by ntsecurity.nu

Linux does not support ADS, although an interesting slack space tool is available called Bmap, which you can download from www.securityfocus.com/tools/1359. This Linux tool can pack data into existing slack space. Anything could be hidden there, as long as it fits within the available space or is parsed up to meet the existing size requirements.

One final step for the attacker is to gain a command prompt on the victim's system. This allows the attacker to actually be the owner of the box. Tools that allow the attacker to have a command prompt on the system include Psexec, Remoxec, and Netcat. Netcat is covered in detail in Chapter 6, "Trojans and Backdoors." After the attacker has a command prompt on the victim's computer, he will usually restart the methodology, looking for other internal targets to attack and compromise. At this point, the methodology is complete. As shown in Figure 4-5, you can see that the attacker has come full circle.

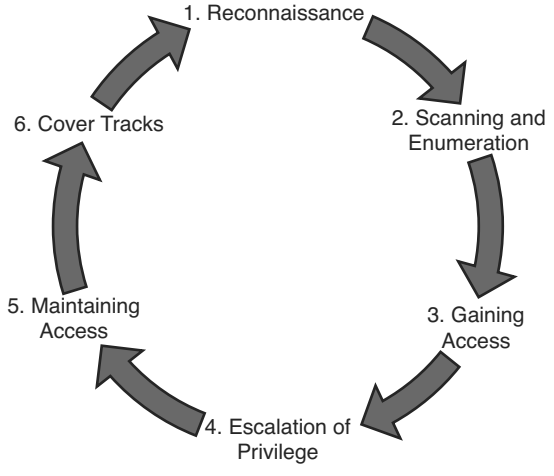

Figure 4-5 Methodology overview.

Chapter Summary

In this chapter, you learned about Windows enumeration and system hacking. Enumeration of Windows systems can be aided by SMB, the `IPC$` share, SMTP, SNMP, and DNS. Each offers opportunities for the attacker to learn more about the network and systems he is preparing to attack. The goal of enumeration is to gather enough information to map the attack surface, which is a collection of potential entry points. It might be a buffer overflow, an unsecure application, such as SNMPv1 or 2, or even a weak password that is easily guessed.

System hacking represents a turning point, which is the point at which the attacker is no longer probing but is actually attacking the systems and attempting to break in. System hacking might start with a low-level account. One key component of system hacking is escalation of privilege, which is the act of exploiting a bug, design flaw, or configuration oversight to gain elevated access. The attacker's overall goal is to own the system. After spending time gaining access, the attacker will want long-term control of the computer or network. After an attacker penetrates and controls one computer, he rarely stops there. He will typically work to cover his tracks and remove any log entries. Besides redirecting sensitive information, stealing proprietary data, and establishing backdoors, attackers will most likely use the compromised system to spread their illegal activities to other computers. If any one system is compromised, the entire domain is at risk. The best defense is a good offense. Don't give the attacker any type of foothold.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here; Chapter 14, "Final Preparation"; and the exam simulation questions on the CD-ROM.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-6 lists a reference of these key topics and the page numbers on which each is found.

Table 4-6 Key Topics for Chapter 4

Key Topic

Key Topic Element	Description	Page Number
Section	Explains how enumeration works	140
Table 4-2	User ID and corresponding RID code	142

Key Topic Element	Description	Page Number
Table 4-3	Microsoft key ports and protocols	143
Section	Explains how system hacking works	151
Section	Explains how ADS works	163

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Active Directory, brute-force attack, dictionary attack, hybrid attack, Inter-Process Communication, kernel, kernel mode, keystroke loggers, local security authority subsystem, NetBIOS, RainbowCrack techniques, relative identifiers, Security Accounts Manager, security identifiers, Server Message Block, Simple Network Management Protocol, and user mode

Command Reference to Check Your Memory

The CEH exam focuses on practical, hands-on skills that are used by a security professional. Therefore, you should be able to identify common `net use` commands.

Table 4-7 `net use` Commands

Task	Command Syntax
Null session	`net use \\ip address\ipc$ "" /u:""`
Map a drive	`net use * \\ip address\share * /u:username`
View open shares	`net view \\ipaddress`

Exercise

4.1 NTFS File Streaming

By using NTFS file streaming, you can effectively hide files in an NTFS environment.

Estimated Time: 15 minutes.

1. Download Sfind and LNS—two good NTFS file streaming programs. Sfind is at www.antiserver.it/Win%20NT/Security/download/ForensicToolkit14.exe, and LNS is at www.ntsecurity.nu/toolbox/lns/.
2. Create a temporary folder on the root of your NTFS drive. Name the folder **test**, or give it another suitable name.
3. Copy notepad.exe into the test folder and rename it **hack.exe**. You will use this file to simulate it as the hacking tool.
4. Next, create a text file called **readme.txt**. Place some text inside the readme file, something like hello world will work.
5. Open a command prompt and change directories to place yourself in the test folder. By performing a directory listing, you should see two files: hack.exe and readme.txt. Record the total free space shown after the directory listing:

   _____
6. From the command line, issue the following command:

```
Type hack.exe > readme.txt:hack.exe
```

7. Now run a directory listing again and record the free space results:

   _____
8. Has anything changed? You should have noticed that free space has been reduced. That is because you streamed hack.exe behind readme.txt.
9. Execute the following from the command line:

```
Start c:\ test\ readme.txt:hack.exe
```

10. Did you notice what happened? Your hacked file, notepad.exe, should have popped open on the screen. The file is completely hidden, as it is streamed behind readme.txt.
11. Finally run both Sfind and LNS from the command line. Both programs should detect the streamed file hack.exe. File streaming is a powerful way to hide information and make it hard to detect.

Review Questions

1. How can you determine whether an LM hash you extracted contains a password that is fewer than eight characters long?
   a. There is no way to tell because a hash cannot be reversed.
   b. The rightmost portion of the hash is always the same.

c. The hash always starts with AB923D.

d. The leftmost portion of the hash is always the same.

2. Which of the following is a well-known password-cracking program?

a. L0phtcrack

b. Netcat

c. Jack the Ripper

d. NetBus

3. What did the following commands determine?

```
C:\  user2sid \ \ truck guest
S-1-5-21-343818398-789336058-1343024091-501
C:\ sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is Truck
```

a. These commands demonstrate that the Joe account has a SID of 500.

b. These commands demonstrate that the guest account has not been disabled.

c. These commands demonstrate that the guest account has been disabled.

d. These commands demonstrate that the true administrator is Joe.

4. What is the RID of the true administrator?

a. 0

b. 100

c. 500

d. 1000

5. What is the best alternative if you discover that a rootkit has been installed on one of your computers?

a. Copy the system files from a known good system.

b. Perform a trap and trace.

c. Delete the files and try to determine the source.

d. Rebuild from known good media.

6. To increase password security, Microsoft added a second layer of encryption. What is this second later called?
   a. Salt
   b. SYSKEY
   c. SYS32
   d. SAM

7. SNMP is a protocol used to query hosts and other network devices about their network status. One of its key features is its use of network agents to collect and store management information, such as the number of error packets received by a managed device. Which of the following makes it a great target for hackers?
   a. It's enabled by all network devices by default.
   b. It's based on TCP.
   c. It sends community strings in cleartext.
   d. It is susceptible to sniffing if the community string is known.

8. Which of the following is the best way to prevent the use of LM authentication of your legacy Windows 2003 servers?
   a. Use the LMShut tool from Microsoft.
   b. Use the NoLMHash Policy by Using Group Policy.
   c. Disable Lsass in Windows 2003.
   d. Use a password that is at least 10 characters long.

9. Which of the following tools can be used to clear the Windows logs?
   a. Auditpol
   b. ELSave
   c. PWdump
   d. Cain and Abel

10. What is one of the disadvantages of using John the Ripper?
    a. It cannot crack NTLM passwords.
    b. It separates the passwords into two separate halves.
    c. It cannot differentiate between uppercase and lowercase passwords.
    d. It cannot perform brute-force cracks.

11. You found the following command on a compromised system:

```
Type nc.exe > readme.txt:nc.exe
```

What is its purpose?

a. This command is used to start a Netcat listener on the victim's system.
b. This command is used to stream Netcat behind readme.txt.
c. This command is used to open a command shell on the victim with Netcat.
d. This command is used to unstream Netcat.exe.

12. Which of the following uses the faster time-memory trade-off technique and works by precomputing all possible passwords in advance?

a. Rainbow tables
b. Dictionary cracks
c. Hybrid cracks
d. Brute-force crack

13. Why would an attacker scan for port 445?

a. To attempt to DoS the NetBIOS SMB service on the victim system
b. To scan for file and print sharing on the victim system
c. To scan for SMB services and verify that the system is Windows 2000 or greater
d. To scan for NetBIOS services and verify that the system is truly a Windows NT server

14. You have downloaded a tool called SYSCracker, and you plan to use it to break SYSKEY encryption. The first thing the tool prompts you for is to set the level of SYSKEY encryption. How many bits are used for SYSKEY encryption?

a. 40 bits
b. 64 bits
c. 128 bits
d. 256 bits

15. You are trying to establish a null session to a target system. Which is the correct syntax?

    a. `net use \\ IP_address\ IPC$ "" /u:""`

    b. `net use //IP_address/IPC$ "" \ u:""`

    c. `net use \\ IP_address\ IPC$ * /u:""`

    d. `net use \\ IP_address\ IPC$ * \ u:""`

Suggested Reading and Resources

www.bindview.com/Services//RAZOR/Utilities/Windows/enum_readme.cfm: Enum website

www.systemtools.com/cgi-bin/download.pl?DumpAcl: DumpSec home page

http://evgenii.rudnyi.ru/programming.html#overview: SID2USER enumeration tools

www.securityfocus.com/infocus/1352: Enumerating Windows systems

www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cnbd_trb_gtvp.asp: NBTStat overview and uses

www.governmentsecurity.org/articles/ExploitingTheIPCShare.php: Exploiting the `IPC$` share

www.netbus.org/keystroke-logger.html: Keystroke loggers

www.theregister.co.uk/2003/03/07/windows_root_kits_a_stealthy: Windows rootkits

www.hnc3k.com/hackingtutorials.htm: Hacking Windows

www.antionline.com/showthread.php?threadid=268572: Privilege/escalation tools